UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Docket No. 20-cr-40036-TSH
	)	
	)	***LEAVE TO FILE REDACTED MEMO***
VINCENT KIEJZO	)	***AND EXHIBITS UNDER SEAL***
	)	***AND TO FILE EXCESS PAGES***
	)	***GRANTED ON 5/24/22***

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The defendant, Vincent Kiejzo, pursuant to Fed. R. Crim. P. 12 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because the warrant was not supported by probable cause. Mr. Kiejzo also moves for a *Franks* hearing, as the affiant made material misstatements that were necessary to a finding of probable cause and omissions that, if included in the affidavit, would have vitiated probable cause.

STATEMENT OF FACTS[1]

I. The Search Warrant

On September 8, 2020, Homeland Security Investigations ("HSI") Special Agent Caitlin Moynihan submitted an application for a search warrant to the U.S. District Court of Massachusetts. *See* Search Warrant Affidavit (attached as Ex. 1). Agent Moynihan sought authorization to search Mr. Kiejzo's home located in Milford, Massachusetts for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Attempted Receipt of

[1] The facts in this section are drawn from the discovery and disclosures provided by the government. By repeating the facts here, Mr. Kiejzo does not adopt them as true.

Child Pornography) and 2252A(a)(5)(B) and (b)(2) (Access with Intent to View and Possession of Child Pornography, and attempt). Ex. 1 at ¶ 4.

The affidavit submitted in support of the search warrant alleged that there was probable cause to believe that a user of the internet account at Mr. Kiejzo's home had accessed, one time each on a single date in May 2019, two Tor hidden-services websites geared towards the sexual exploitation of minors. Agent Moynihan identified the sites as Website 2 and Website 3 in her affidavit. Specifically, regarding Website 2, Agent Moynihan stated:

> In August 2019, a foreign law enforcement agency (hereinafter, "FLA") known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that the FLA had determined that on May 12, 2019 at 19:10:51 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2.

Id. at ¶ 31. Agent Moynihan stated that the "FLA described the website as having an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore, and death-related material including that of children." *Id*. She noted that "[u]sers were required to create an account (username and password) in order to access the majority of the material." *Id*. She also stated that the "FLA provided further documentation naming the site…as Website 2".[2] *Id*.

The information in the affidavit regarding the alleged visit to Website 3 was nearly identical. It read: "In August 2019, FLA notified U.S. law enforcement that FLA had determined that on May 12, 2019 at 19:27:24 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 3." *Id*. at ¶ 32. Agent Moynihan relayed the FLA's description of Website 3 as having "an explicit

[2] Agent Moynihan noted in the affidavit that the FLA "referred to the site by its actual name." Ex. 1 at ¶ 31. The government has since disclosed that the website was called [redacted]

focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys." *Id*. Agent Moynihan also stated that the FLA reported "users were able to view some material without creating an account," but that "an account was required to post and access all content."[3] *Id*. The affidavit did not include any allegations that the suspect user IP address was used to create an account on either website, nor did it include any information about exactly what material was allegedly "accessed" on the websites. Agent Moynihan did not state what section of the websites the internet user associated with that IP address had visited, if any, nor whether the suspect user had navigated past the homepage of either website.

With respect to Website 2, Agent Moynihan claimed that it was an "online bulletin board dedicated to the advertisement and distribution of child pornography" that operated from at least September 2016 to June 2019. *Id*. at ¶ 15. Agent Moynihan stated that in "June of 2019, the computer server hosting Website 2, which was located outside of the United States, was seized by a foreign law enforcement agency." *Id*.

Similarly, Agent Moynihan described Website 3 as "an online forum dedicated to the sexual exploitation of minor and/or prepubescent males." *Id*. at ¶ 23. That website, according to Agent Moynihan, began operating in 2013 and, like Website 2, ceased operation in June 2019 when "the computer server hosting Website 3, which was located outside of the United States, was seized by a foreign law enforcement agency." *Id*.

Agent Moynihan explained that Websites 2 and 3 were "hidden service" websites that operated on the Tor network, a free and legal computer network "available to internet users that is designed specifically to facilitate anonymous communication over the internet." *Id*. at ¶ 7, 12.

[3] Agent Moynihan noted in the affidavit that the FLA referred to Website 3 "by its actual name." Ex. 1 at ¶ 32. The government has since disclosed that the website was called [redacted]

Agent Moynihan also included a description of how the Tor network operates and how information is anonymized on the network, noting that "the Tor network attempts to [facilitate anonymous communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit.'" *Id*. at ¶ 7. Agent Moynihan acknowledged that because of this process, "traditional IP address-based identification techniques are not effective," but she neither expounded on the methodology used to identify the suspect user IP address in this case, nor provided any explanation for the reliability of the identification of the suspect user IP address. *Id*.

In the section of the affidavit discussing the FLA tips, Agent Moynihan claimed that the FLA (later identified by the government in response to defense discovery requests as the [redacted] was a "national law enforcement agency of a country with an established rule of law." *Id*. at ¶ 33. Agent Moynihan averred that there was a "long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." *Id*. Agent Moynihan also stated that the FLA "had obtained that [tip] information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." *Id*. She further noted that the FLA had "advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information." *Id*. She stated that "U.S. law enforcement did not participate in the investigative work through which FLA identified the IP address." *Id*.

Finally, Agent Moynihan alleged that prior tips provided by the FLA had:

> (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further

> investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

Id. at ¶ 34.

According to the affidavit, in March 2020, U.S. law enforcement sent a subpoena to Verizon Fios for subscriber information related to the suspect user IP address. *Id*. at ¶ 39. Verizon provided law enforcement with a physical address – [redacted] – associated with the IP address as well as the customer name – Alexander Kiejzo. *Id*. Agent Moynihan stated that commercial databases, RMV records, and USPS records indicated that Alexander Kiejzo lived at that address and that his son, Vincent Kiejzo, received mail there. *Id*. at ¶ 40-42. Agent Moynihan also noted that on September 4, 2020 and September 8, 2020, officers conducting surveillance observed two men who resembled Alexander and Vincent at the subject premises. *Id*. at ¶ 43-44. Agent Moynihan also stated that Vincent Kiejzo had been issued a firearms identification card in May 2017, which listed [redacted] has his residential address. *Id*. at ¶ 45. Agent Moynihan included the fact that officers found a LinkedIn page indicating that Vincent Kiejzo listed his employment as a second grade teacher at Milford public schools. *Id*. at ¶ 46. Finally, Agent Moynihan noted that while parked in front of [redacted], two wireless networks were available and they were named KIEJZO and KiejzoSH. *Id*. at ¶ 47.

A warrant to search Mr. Kiejzo's home was issued on September 8, 2020. *See* Search Warrant (attached as Ex. 2). The warrant was executed the next day. Based on the evidence discovered at Mr. Kiejzo's home, Mr. Kiejzo was arrested and a complaint was filed alleging a violation of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography). Mr. Kiejzo was later indicted on one count of possession of child pornography.

II. Information Omitted from the Affidavit

In response to specific defense discovery requests, the government disclosed that the FLA that provided the tip to U.S. law enforcement (now known to be [redacted]) and the FLA that seized the server that hosted Websites 2 and 3 were not just different FLAs, but from different countries altogether. The government further disclosed that the FLA that seized the server was local to the server host country (not [redacted]). The government has declined to identify the second FLA or the server host country.

Since that disclosure, the defense has uncovered additional information not included in Agent Moynihan's affidavit that is material to the probable cause analysis. First, undersigned counsel have identified multiple cases from across the country that rely on seemingly identical August 2019 tips from an undisclosed FLA that an IP address was used to visit a Tor hidden services website sometime in April or May 2019. *See* Ex. 10-16. The number of similar cases using similar, if not identical, language to the search warrant affidavit in Mr. Kiejzo's case indicates a large-scale, coordinated investigation into websites hosted on the Tor network akin to the Playpen investigation.[4]

Second, documents from a variety of sources indicate that U.S. law enforcement was investigating Tor hidden websites, including Website 2 [redacted], years before receiving the tip from [redacted]. For example, an FBI report dated January 13, 2017 documents a "preliminary investigation" into a Tor hidden service site with language identical to that found on [redacted]. *See* Ex. 18. This FBI report indicates that U.S. law enforcement opened an investigation into [redacted] more than two years before [redacted] relayed its "tip" that the suspect IP address had purportedly visited [redacted]. Other documents indicate that Homeland Security – HSI Boston in particular – was investigating the websites as early as 2016. *See* Ex. 19, 20.

[4] *See* "The Playpen Cases: Mass Hacking by U.S. Law Enforcement," Electronic Frontier Foundation, available at https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement.

Third, a set of recently obtained documents show that there was a large-scale, coordinated investigation into specific Tor hidden websites conducted as a joint venture between U.S. and foreign law enforcement agencies, a highly significant fact that Agent Moynihan withheld from her affidavit. In particular, documents from the Canadian criminal case against the creator of [redacted] indicate that Homeland Security – as early as 2016 – was engaged in a joint investigation of Tor websites that hosted child abuse materials, *including* [redacted], with law enforcement agencies in New Zealand and Canada.[5] *See* Ex. 19, 20. Court documents in other U.S. District Courts also specifically describe the U.S. investigation into Tor-hidden websites as collaborative with foreign law enforcement partners. *See* Ex. 13. In fact, this collaboration between U.S. and foreign law enforcement agencies was significant enough that U.S. law enforcement was in possession of a searchable copy of [redacted] (Website 2) – something it would have obtained from the FLA that seized the server hosting [redacted] – in January 2020, eight months before law enforcement sought a warrant in this case. *See* Ex. 16.

None of this information was included in Agent Moynihan's affidavit.

ARGUMENT

I. The Warrant Was Not Supported By Probable Cause.

The Fourth Amendment of the United States Constitution guarantees the right to be secure against "unreasonable searches and seizures" and requires that no warrants issue "but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched." U.S. Const. Am. IV. "With limited exceptions, it requires police officers to secure a

[5] [redacted]

search warrant supported by probable cause prior to effecting a search or seizure." *United States v. Gifford*, 727 F.3d 92, 98 (1st Cir. 2013).

Probable cause to issue a search warrant exists when "given all the circumstances set forth in the affidavit … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id*. at 239. This Court is tasked with "ensur[ing] that the magistrate had a substantial basis for ... concluding that probable cause existed." *Id*. at 238-39.

When an affidavit relies on information provided by a confidential informant, "the affidavit must provide some information from which a magistrate can credit the informant's credibility." *Gifford*, 727 F.3d at 99. The First Circuit applies the following non-exhaustive factors in assessing probable cause in cases involving confidential tips:

> (1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant's statements reflect first-hand knowledge; (3) whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant's provided information.

United States v. Tiem Trinh, 665 F.3d 1, 10 (1st Cir. 2011).

Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Kiejzo's home. *Gates*, 462 U.S. at 238-39. The affidavit relied entirely on two unsubstantiated and stale allegations of criminal activity by an unidentified foreign law enforcement agency (now known to be [redacted]). The affidavit failed to include any information as to how the FLA came across that information, how

reliable the method the FLA used to obtain the information was (if indeed it was that FLA that de-anonymized the suspect user IP address here), and whether the IP address and/or other tip information was obtained through the FLA's first-hand knowledge or through other sources. Without more information about the source of the FLA's tip and without additional corroboration, the sixteen-month-old tip was not sufficient to establish probable cause.

a. The FLA Tip Was Insufficient To Establish Probable Cause.

The factors outlined by the First Circuit in *Tiem Trinh*, 665 F.3d at 10, are instructive in this case because the tip that forms the entire basis of probable cause in the affidavit came from a confidential source akin to an informant. Those factors, although non-exhaustive, weigh in Mr. Kiejzo's favor. Agent Moynihan's affidavit is deficient because 1) it fails to establish the basis of knowledge for the tip and whether it was obtained through first-hand knowledge or through hearsay (factors 1 and 2 in the *Tiem Trinh* analysis), and 2) it reflects no attempts from any U.S. law enforcement agency to corroborate the tip from the unidentified FLA (factor 3 of *Tiem Trinh*).

i. The Affidavit Fails to Establish the Basis of Knowledge for the Tip.

The affidavit is deficient because it failed to establish the basis of knowledge for the tip in two respects. First, Agent Moynihan did not include any information about whether the tip was obtained through first-hand knowledge or through hearsay. Second, Agent Moynihan included no facts about the method used to obtain the IP address information and whether that method was reliable.

The only information provided in the affidavit that offered any clues about the source of the FLA's tip were Agent Moynihan's statements that the FLA "had obtained [the information in the tip] through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws," and that "FLA had not interfered with, accessed, searched, or seized any data

from any computer in the United States in order to obtain that IP address information." Ex. 1, ¶ 33. However, neither statement by Agent Moynihan was sufficient to establish or to assure the Magistrate of the tip's reliability. Agent Moynihan did not state that the IP address information had reached the FLA through a reliable first-hand source rather than through multiple layers of hearsay. *Cf. Gates*, 462 U.S. at 234 (noting that the informant's "explicit and detailed description of alleged wrongdoing, along with a statement that the event was observed *first-hand*, entitles his tip to greater weight than might otherwise be the case"); *United States v. Taylor*, 985 F.2d 3, 5-6 (1st Cir. 1993) (noting that an affidavit may support an informant's veracity "through the very specificity and detail with which it relates the informant's *first-hand* description of the place to be searched or the items to be seized"). Nor did Agent Moynihan aver that *no* FLA had "interfered with, accessed, searched, or seized any data from any computer in the United States."[6] Ex. 1, ¶ 33. Instead, Agent Moynihan left the Magistrate to guess at how the FLA had obtained the information and to merely ratify Agent Moynihan's conclusion that the tip was a reliable one.

The First Circuit has found that a lack of explanation of the basis of knowledge for an informant's tip undermines a finding of probable cause. *Gifford*, 727 F.3d at 99-101. In *Gifford*, an informant told the affiant that the defendant was growing marijuana at his house. *Id*. at 95. However, the affidavit included no information about the informant's basis of knowledge for the tip. It was therefore unclear "whether the informant just happened to view the grow operation, heard about it as hearsay, or had direct, first-hand knowledge of the grow operation in the Gifford home." *Id*. at 100. Because the affidavit lacked any "statements as to the informant basis of knowledge," there was no means for the magistrate to determine "whether that information was

[6] This is especially important given what was later disclosed relative to a second FLA that actually seized the server, and was involved at an earlier stage of the investigation.

obtained first-hand or through rumor." *Id*. The lack of any information about the source of the informant's knowledge weighed against a reliability finding in *Gifford*.

The facts of this case mirror those in *Gifford* and compel the same conclusion. As in *Gifford*, it is entirely unclear how, when, and through what method the FLA that provided the tip learned about the IP address. Without that information, there was no basis for the magistrate to determine whether the content of the tip from the FLA was reliable and trustworthy. By not divulging any information about the FLA's basis of knowledge, the magistrate was left with no reason to believe that the tip was obtained through a reliable and trustworthy source or method. Simply repeating the FLA's allegation without further explaining how the FLA uncovered the connection between the IP address and the accessing of child sexual abuse material was insufficient to adequately establish the basis of knowledge of the tip. Thus, the first and second factors of *Tiem Trinh* – "whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information" and "whether an informant's statements reflect first-hand knowledge" – weigh in Mr. Kiejzo's favor. *Tiem Trinh*, 665 F.3d at 10.

ii. The Affidavit Reflects No Effort From Law Enforcement To Corroborate the Substance of the Tip.

In addition to the lack of information about the basis of knowledge or reliability of the method used to obtain the IP address, the affidavit does not include any facts that actually or meaningfully corroborated the tip from the FLA that an internet user had "accessed online child sexual abuse and exploitation material via a website." Ex. 1, ¶ 31-32. While Agent Moynihan did include a description of the steps U.S. law enforcement took to confirm who lived at 17 Joan Circle, that investigation only corroborated the fact that someone lived at the physical address associated with the IP address identified by the FLA. None of that investigation corroborated the tip that that particular IP address was used to access child abuse material on May 12, 2019.

In the affidavit, Agent Moynihan briefly detailed the steps agents took to identify who, if anyone, lived at [redacted]. Agents learned, according to the affidavit, that Vincent Kiejzo received mail at that address and that it was listed as his address on his driver's license. *Id*. at ¶ 40-42. Agents saw an individual who looked like Mr. Kiejzo leave the house on September 8, 2020. *Id*. Finally, Agent Moynihan noted that Mr. Kiejzo was issued a Firearms ID card in May 2017, which designated his address as [redacted]. *Id*. at ¶ 45.[7]

While this information certainly may have substantiated a claim that Mr. Kiejzo lived at that address in September 2020, none of it corroborated the allegation made by the FLA – that an internet user at [redacted] had accessed child sexual abuse material in May 2019. *See Gifford*, 727 F.3d at 99-102 (DMV records that confirmed the defendant lived at his address did not corroborate an informant's tip that there was an ongoing grow operation at that address). There was no evidence in the affidavit that the Internet user had any interest in child pornography other than an uncorroborated allegation of a single visit to an unknown part of two target websites, which, as argued below, is not enough to demonstrate an interest in such material. The affidavit contains no information actually corroborating the unreliable tip from the FLA. The third factor identified in *Tiem Trinh* – "whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable" – therefore weighs in favor of Mr. Kiejzo. *Tiem Trinh*, 665 F.3d at 10.

In sum, Agent Moynihan failed to establish the basis of knowledge for the tip or the reliability of the method used to obtain the information in the tip. Agent Moynihan also failed to include any facts that corroborated the unreliable tip. The information provided in the affidavit

[7] Agent Moynihan stated that Alexander Kiejzo, Vincent Kiejzo's father, also lived at the residence. Ex. 1, ¶ 39-43.

therefore did not create a "substantial basis" for the magistrate to conclude that probable cause existed. *Gates*, 462 U.S. at 238-39.

b. The Warrant Was Stale.

Stale information cannot establish probable cause that evidence of criminal activity will be found at the place searched. *United States v. Grubbs*, 547 U.S. 90, 96 n.2 (2006). Whether information is stale does not depend solely on the number of days between the events described in the affidavit and the issuance of the warrant. *Tiem Trinh*, 665 F.3d at 13–14. Courts look instead at a number of factors, including "the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." *Id.* (citing *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008)). In cases involving child pornography, courts have often determined that the passage of a significant amount of time between the acquisition of the incriminating information and the obtaining of a warrant does not render the information stale where the magistrate was provided with information supporting a finding that such materials are likely to have been retained by their possessor. *See, e.g., Morales-Aldahondo*, 524 F.3d at 119.

Here, the FBI did not have probable cause to search Mr. Kiejzo's home in September 2020 when the alleged access to child sexual abuse material occurred in May 2019 – sixteen months earlier. The affidavit did not include any allegations specific to Mr. Kiejzo regarding any propensity or habits of keeping a collection of child pornography. Moreover, the affidavit failed to state what exactly was accessed on the website, whether it was downloaded or saved in any manner, or whether there were multiple visits to the website – facts that might have bolstered probable cause. *Cf. United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015) (no probable cause where the affidavit alleged only that "on a single afternoon more than nine months earlier, a user

with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files").

Without more information specific to Mr. Kiejzo, and without more information about the material allegedly viewed by the suspect user IP address, there was not probable cause to believe that Mr. Kiejzo's home contained evidence of a crime. Not only was the sole criminal allegation in the warrant sixteen months old, but any information about the reliability and source of that allegation was absent from the affidavit. The uncorroborated, stale, and unreliable tip was insufficient to establish probable cause. The warrant was unlawfully issued, and all evidence obtained as a result of the search conducted pursuant to the warrant must be suppressed.

II. The Affiant Made Material Omissions and Misstatements and Mr. Kiejzo is Entitled to a *Franks* Hearing as a Result.

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *Gifford*, 727 F.3d at 98 (internal quotations omitted). "Suppression of the evidence seized is justified if, at such a hearing, the defendant proves intentional or reckless falsehood by preponderant evidence and the affidavit's creditworthy averments are insufficient to establish probable cause." *United States v. Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015).

The right to a Franks hearing is triggered not only by false statements but also by material omissions. *Id.*; *United States v. Cartagena*, 593 F.3d 104, 112 (1st Cir. 2010). When a defendant alleges a material omission has been made, "[t]he required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. The First Circuit has held that recklessness may be inferred where "the omitted information was critical to the probable cause determination." *Gifford*, 727 F.3d at 98-100.

Special Agent Moynihan made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth, regarding four key issues. First, Agent Moynihan made material misstatements about the nature, origin, and reliability of the tip from the FLA. Second, Agent Moynihan made material omissions about the method(s) used by the FLA to identify the IP address. Third, Agent Moynihan's explanation of Tor was misleading. Fourth, Agent Moynihan misrepresented the relationship between U.S. law enforcement and the FLA(s) in the affidavit. Each of these misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause. Mr. Kiejzo is therefore entitled to a *Franks* hearing.

a. Agent Moynihan Misrepresented the Nature, Origin, and Reliability of the Tip.

Agent Moynihan's affidavit relies entirely on her assertion that an FLA notified U.S. law enforcement that a particular IP address twice "was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2 [and Website 3]." Ex. 1, ¶ 31-32. There are no other allegations of criminal activity anywhere in the affidavit. However, this fact is inherently misleading and factually incorrect. Agent Moynihan did not repeat

the tip from the [redacted] verbatim. Rather, she added language that misled the magistrate into believing that U.S. law enforcement had more evidence of criminal activity that it did.

The exact words of the tip relayed from the [redacted] to U.S. law enforcement regarding Website 2 were:

> On 2019-05-12 19:10:51 (UTC) 96.230.213.63 was used to access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links, and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children. Users were required to create an account (username and password) in order to access the majority of the material[.]

See Ex. 3. Agent Moynihan did not copy or repeat this language into the affidavit. Instead, she stated the following in her affidavit:

> [FLA] notified U.S. law enforcement that the FLA had determined that on May 12, 2019 at 19:10:51 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material **via a website** that the FLA named and described as Website 2. FLA described the website as having an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore, and death-related material including that of children, stated that users were required to create an account (username and password) in order to access the majority of the material[.]

Ex. 1, ¶ 31 (emphasis added).

Agent Moynihan made the same change in relation to the tip regarding Website 3. The tip from the [redacted] stated:

> On 2019-05-12 19:27:24 (UTC) 96.230.213.63 was used to access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse materials (images, links and videos), emphasis on indecent material of boys. Users were able to view some material without creating an account. However, an account was required to post and access all content.

Ex. 3. As with Website 2, Agent Moynihan did not repeat this tip verbatim. The affidavit states:

> In August 2019, FLA notified U.S. law enforcement that FLA had determined that on May 12, 2019 at 19:27:24 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material **via a website** that the FLA named and described as Website 3. FLA described the website as having "an

> explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys," stated that "[u]sers were able to view some material without creating an account. However, an account was required to post and access all content[.]

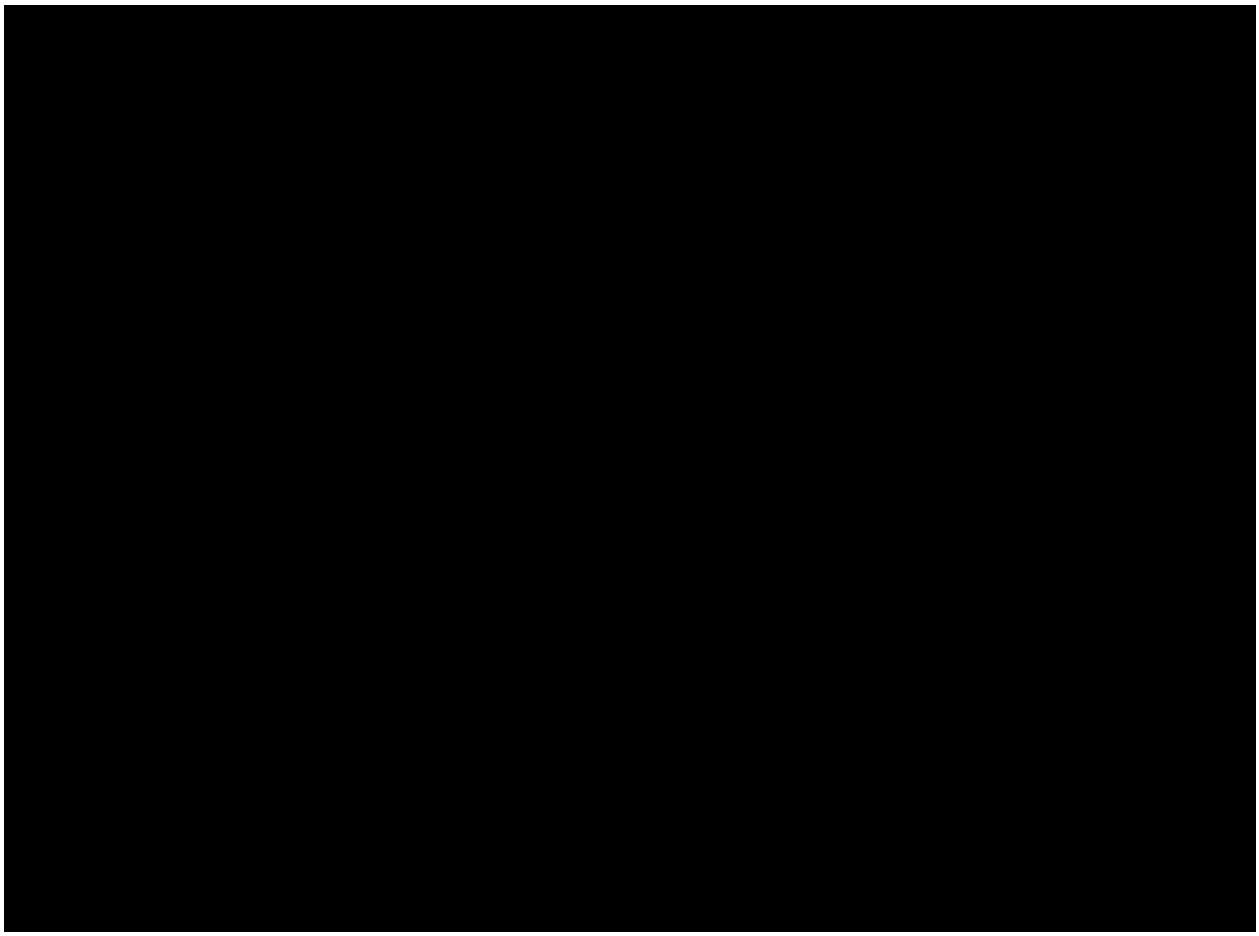
Ex. 1, ¶ 32 (emphasis added).

While these changes may appear slight, their significance in the affidavit was profound. By manipulating the language of the tip, Agent Moynihan created the impression that the [redacted], and therefore U.S. law enforcement, had information that the IP address was used to visit Website 2 and Website 3 *and then used to access child sexual abuse material*. The implication in the affidavit is that the internet user associated with that IP address viewed or downloaded the child sexual abuse material available on Website 2 and Website 3 and possibly that, because the majority of the material was only available through an account, the internet user indeed had such an account and had accessed the child sexual abuse material through that account. However, this wholly misrepresents the substance of the tip from the [redacted]. The [redacted] did not provide any such information, nor did U.S. law enforcement have any such evidence. Rather, the tip from the [redacted] conveyed only that the IP address in question was merely used to *access the websites*.

Other documents disclosed by the government support this interpretation of the tip. In the Intelligence Report, the [redacted] states that the IP address was used to "access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material." Ex. 3. The tip is inscrutable as it is written because it is unclear how "child sexual abuse and exploitation material" (i.e., videos and images) can have an "explicit focus" on the *facilitation of sharing the same material*. Its meaning only becomes clear if the phrase "online child sexual abuse and exploitation material" in the first clause means Websites 2 and 3, rather than images or videos depicting child sexual abuse. In other words, the Intelligence Report, and therefore the affidavit, should be read as "On 2019-05-12 19:10:51 (UTC) 96.230.213.63 was used to access

[Website 2], with an explicit focus on the facilitation of sharing child abuse material (images, links, and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children." *See* Ex. 1, ¶ 31. The same goes for the tip regarding Website 3. It should be read as "On 2019-05-12 19:27:24 (UTC) 96.230.213.63 was used to access [Website 3], with an explicit focus on the facilitation of sharing child abuse materials (images, links and videos), emphasis on indecent material of boys."

This reading is consistent with, and tracks the exact language of, the [redacted] Intelligence Report identifying the website. That report uses the identical language to describe the *website itself*, not the activity of the internet user:



Ex. 5.[8] Comparing the language of the report from the [redacted] to the words Agent Moynihan used in her affidavit, it is clear that Agent Moynihan misrepresented what information the [redacted] actually relayed to U.S. law enforcement.

Other parts of the affidavit reflect that the [redacted] original tip – that a specific IP address was used to **access a website**, not material on that website – was and has been, U.S. law enforcement's understanding of the [redacted] tip. *See* Ex. 1 at ¶ 5 ("There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES **accessed Website 2 and Website 3**."); p. 15 ("Evidence Related to Identification of Target that **Accessed Website 2 and Website 3**"); ¶ 39 ("According to publicly available information, IP address 96.230.213.63 — **the one used to access Website 2 and Website 3**, as described above — is owned/operated by Verizon Fios.").

In altering the language from the [redacted] tip, Agent Moynihan also omitted the crucial fact that the homepages of Websites 2 and 3 did not display any child sexual abuse material. Screenshots of the website provided by the government show that in order to "access" any child sexual abuse material, an individual would have had to navigate past the homepages of both websites. *See* Ex. 6, 7. Neither the tip documents nor Agent Moynihan's affidavit specify what, if any, images, videos, or other materials were viewed, downloaded, or "accessed" in any way. Neither the tip documents nor the affidavit state whether the suspect user IP address did anything beyond accessing the homepages, which contained no contraband images or material. Neither the tip documents nor the affidavit allege that the individual associated with the IP address had an account on either website, or that that account was used to "access" any materials. In sum, Agent Moynihan mischaracterized the substance of the tip from the [redacted], which was solely that the IP

[8] The images and videos named in Ex. 5 appear to be those shared on the website, not those accessed, viewed, or downloaded by any one user, let alone Mr. Kiejzo. Similarly, the excerpted descriptions in the affidavit of particular images found on Website 2 or 3, *see* Ex. 1 at ¶ 21-22, 28-29, are not alleged to have been accessed, viewed, posted or downloaded by Mr. Kiejzo.

address in question was used to access Websites 2 and 3, neither of which displayed any child sexual abuse images or videos on its homepage.

The distinction between the substance of the tip and Agent Moynihan's rewording of that tip in the affidavit is important. There is a fundamental difference between: 1) evidence of a one-time visit to a website where no images, videos, or links to child pornography materials were either visible or available on the website's homepage, and no such items were viewed and/or downloaded and 2) evidence of an individual accessing that website and then viewing, downloading, or otherwise possessing materials that would have only been accessible once a user navigated past the homepage. *See United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website—which did not require registering an account or logging in—and that even if one inferred that the defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"); *Raymonda*, 780 F.3d at 105. The information the [redacted] relayed to U.S. law enforcement fell squarely into the first category, which, like *Falso*, was insufficient to establish probable cause.

By manipulating the language in the tip from the [redacted], Agent Moynihan misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did. Agent Moynihan's misrepresentation about the nature of the tip was recklessly made and was "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155-56. Had Agent Moynihan been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used to visit two websites where no child pornography was visible or available on the homepage, the

magistrate could not have found sufficient probable cause to issue the warrant. Mr. Kiejzo is therefore entitled to a *Franks* hearing on these false and misleading statements.

In addition to this misrepresentation about the nature of the tip from the [redacted], Agent Moynihan also omitted important information about the origin and reliability (or lack thereof) of the FLA tip. Specifically, Agent Moynihan stated that that FLA (now known to be [redacted]) had "a history of providing reliable, accurate information in the past" and that it was "a national law enforcement agency of a country with an established rule of law." Ex. 1, ¶ 31, 33. Agent Moynihan averred that the FLA (the [redacted]) had obtained the information in the tip through an investigation that was "lawfully authorized in FLA's country pursuant to its national laws," and that the FLA [redacted] had not "interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information." *Id*. at ¶ 33. Finally, Agent Moynihan claimed that prior tips from the FLA [redacted] had led to an arrest, the rescue of children subject to abuse, and the seizure of evidence. *Id*. at ¶ 34.

However, Agent Moynihan omitted from the affidavit the fact that there was not just one FLA involved in the investigation of Website 2 and 3, but two, from two entirely different countries. The [redacted], which provided the tip to U.S. law enforcement and which Agent Moynihan took pains to assure the court was subject to the rule of law, was seemingly not involved in the seizure of the website's server. Instead, the government later disclosed (in response to a defense discovery request) that a second FLA – which it has refused to name – seized the server in a country distinct from [redacted] – a country which it has also refused to name. Additional information – such as who participated in the seizure and what investigative steps were undertaken by the seizing FLA alone or in conjunction with other countries and/or law enforcement, including the United States

– remains unknown. What little *is* known about the second FLA is that it was local to the server host country, which, again, is distinct from [redacted]

Agent Moynihan made no distinction between the two FLAs in the affidavit and failed to inform the court that there was even a second FLA involved in the investigation. Instead, Agent Moynihan created the impression that the tip and the source of that tip both originated from the same, allegedly reliable FLA. This impression was both misleading and inaccurate. While Agent Moynihan made a number of claims in the affidavit about the reliability of the FLA, those statements applied *only* to the FLA that provided the tip to U.S. law enforcement (again, the [redacted]). There are no facts in the affidavit that address or establish the reliability, trustworthiness, or history of prior tips from the FLA that seized the server. Agent Moynihan did not, for example, make any assurances that the FLA that *seized* the server had a "history of providing reliable, accurate information." Nor did Agent Moynihan aver that the second FLA was from a country with an "established rule of law." Ex. 1, ¶ 31, 33. Likewise, there are no facts in the affidavit that could have assured the Magistrate that the FLA that seized the server did not conduct a search or seizure of any computer in the United States (e.g. performing a so-called "Network Investigative Technique" (NIT)).

This misinformation went to the heart of the probable cause analysis. The manipulated tip from the [redacted] was the only allegation of criminal activity in the entire affidavit. It was also the only piece of information that created a nexus between Mr. Kiejzo, his home, and the alleged criminal activity. The omitted fact that there was a second FLA involved in obtaining the IP address information "require[s] that [this Court] alter in significant ways the weight [it] give[s] to" the tip. *Gifford*, 727 F.3d at 101. Without assurances in the affidavit about the reliability and

trustworthiness of the second FLA and the legality of its action, no Magistrate could find there was probable cause.

Because Agent Moynihan's misrepresentations and omissions regarding the nature, origin, and reliability of the tip were all "critical to the probable cause determination," this Court "may infer recklessness" on the part of Agent Moynihan. *Gifford*, 727 F.3d at 101. The reckless misrepresentations were "necessary to the finding of probable cause" and the omitted information, added back into the affidavit, "is sufficient to vitiate probable cause." *Franks*, 438 U.S. at 155-56; *Tanguay*, 787 F.3d at 49. Mr. Kiejzo is therefore entitled to a *Franks* hearing.

b. Agent Moynihan Made Material Omissions Regarding The Method Used by the FLA to Identify the IP Address.

Agent Moynihan's affidavit indicated that the FLA (the [redacted]) assured U.S. law enforcement that that FLA had not "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. 1, ¶ 33. This assurance created the impression that no law enforcement agency, anywhere, had "interfered with, accessed, searched, or seized" data from a computer in the United States. However, an expert declaration submitted in a case seemingly identical to Mr. Kiejzo's, and arising out of the same FLA tip and investigation, suggests that the specific IP address could not have been identified without running a NIT or, in the alternative, an error-prone and unreliable traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2 (attached as Ex. 8). In Professor Murdoch's declaration, he explains that "there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a Network Investigative Technique (which interferes with a user computer)." Ex. 8, ¶ 23. A NIT works "by forcing the user's computer to disclose its IP address by connecting

directly to a law-enforcement server without using the Tor network." *Id*. at ¶ 27. A NIT "necessarily interferes with a user's computer wherever it is located." *Id*. at ¶ 32.

Traffic analysis, on the other hand, is a technique that attempts to "identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." *Id*. at ¶ 17. Before 2016, "traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases." However, in 2016, Tor addressed this issue and introduced a new extension to its software that caused traffic analysis to "introduce more errors, both false positives (where a user is incorrectly identified as having visited the Onion Service) and false-negatives (where a user is incorrectly identified as not having visited the Onion Service)." *Id*. at ¶ 19. This measure, and others, have made it "even more difficult to use traffic-analysis to de-anonymize Tor users." *Id*. at ¶ 21.

The use of either technique by the [redacted] or another FLA would significantly undermine the veracity of the affidavit and its probable cause showing. If traffic analysis were used to uncover the IP address, the undisclosed fact that that technique is inherently error-prone would significantly undermine the strength and reliability of the tip from the [redacted]. *See id*. at ¶ 22-32. No magistrate, had he or she been aware that this fundamentally unreliable technique was used to obtain the IP address, would find there was probable cause, especially where the tip about the IP address was not corroborated by any other facts.

Alternatively, the use of a NIT would reveal a substantial misrepresentation in the affidavit, which relies on Agent Moynihan's assurance that no computer in the United States had been searched. The deployment of a NIT is an unlawful warrantless search. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass.

2016), *aff'd*, 923 F.3d 1 (1st Cir. 2019). Had any law enforcement agency deployed a NIT to obtain the IP address without a warrant, the Magistrate could not have considered the results of that search in the probable cause analysis. *See United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005) ("[W]hen faced with a warrant containing information obtained pursuant to an illegal search, a reviewing court must excise the offending information and evaluate whether what remains is sufficient to establish probable cause.").

Agent Moynihan's omissions regarding the method used to obtain the IP address were material because if the omitted information – either that a NIT or an error-prone traffic analysis was used – was included in the affidavit, it would be "sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100. Mr. Kiejzo is therefore entitled to a *Franks* hearing on this issue as well.

c. Agent Moynihan's Explanation of Tor Was Misleading.

In the affidavit, Agent Moynihan included an explanation of the Tor network and its "unique technical features." Ex. 1, ¶ 7-14. In particular, Agent Moynihan claimed:

> Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion."… Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Users utilize those directory sites to identify new web forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. While they operated, the web addresses for Websites 2 and 3 were listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

Ex. 1, ¶ 13-14.

An affidavit recently filed in another case stemming from the same investigation directly undermines Agent Moynihan's assertions. *See United States v. Stuart*, 21-cr-00007 (W.D.N.Y. Jan. 31, 2022) (Affidavit of Gerald R. Grant) (attached as Ex. 9). The affidavit, written by an expert in computer forensics, explains that "[w]hile it is true that websites on the Tor network are not directly 'indexed' by search engines - such as Google - in the same manner as websites on the public internet, that does not mean that a user cannot easily find links to hidden Tor websites through Google." Ex. 9 at ¶ 4. The expert affidavit specifically notes that a "simple search" can lead to web pages that contain links to hidden Tor websites. *Id*. at ¶ 5. Therefore, "it is possible for a user to easily find a list of links to hidden Tor websites, click on a link, and be taken to that website **without being aware of what content it contains**. The typical names of these hidden Tor websites do not indicate possible content, due to the use of the 16-or-56-character web address." *Id*. at ¶ 6 (emphasis added).

Agent Moynihan's description of Tor hidden services websites, and Websites 2 and 3 in particular, as only accessible if specifically sought out, was therefore misleading. As the Grant affidavit indicates, an individual could easily click on a link to a Tor website and access that website without being aware that the website contains child sexual abuse material. Including such misleading information in the affidavit was a material misrepresentation. This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100. Mr. Kiejzo is entitled to a *Franks* hearing as a result.

d. Agent Moynihan Misrepresented the Nature Of The Relationship Between U.S. Law Enforcement and the FLAs and Omitted Facts That Would Have Revealed that the FLAs' Actions Were Subject to the Exclusionary Rule.

Agent Moynihan's final misrepresentations involved omitting facts about the role of U.S. law enforcement in the investigation of Websites 2 and 3. Specifically, Agent Moynihan withheld information that would have shown that 1) U.S. law enforcement was engaged in a "joint venture" with the FLAs and 2) the FLAs engaged in conduct that would shock the judicial conscience such that the FLAs' actions would be subject to the exclusionary rule.

Generally, "the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). There are, however, two exceptions to that rule: "(1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*. Here, both exceptions would apply to the conduct of the FLAs. Running a NIT to obtain an IP address of a computer in the U.S. – conduct that is unlawful in the U.S. without first obtaining a warrant – and then hiding that information from a magistrate judge would "shock the judicial conscience." *Id*. Likewise, the information available to the defense suggests that there was a "joint venture" afoot between the United States and the FLAs such that the exclusionary rule would apply to one (or both) of the FLAs running a NIT on a computer in the United States. *See id*. However, Agent Moynihan minimized the collaborative relationship between the agencies and withheld facts that would have established that "American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*.

The clearest indication that U.S. law enforcement was engaged in a joint venture with foreign law enforcement agencies comes from the international investigation and resulting

criminal case [redacted] *see also* *United States v. Benjamin Faulkner and Patrick Falte*, Case No. 3:17-CR-00049-JAG (E.D. Va., Oct. 4, 2016) (Criminal Complaint) (attached as Ex. 21).[9] These individuals were arrested and interviewed in the United States. Ex. 19 at 5; Ex. 21 at ¶ 9. During those interviews with U.S. law enforcement agents, Faulkner or Falte, or both, provided "passwords to devices, … encryption keys and signature keys." [redacted] see also Ex. 21 at ¶ 9.

As part of the joint investigation into these websites, HSI then shared the information it had obtained from Faulkner and/or Falte with foreign law enforcement agencies. In particular, HSI immediately sent the usernames, passwords, and encryption keys to the Tor site Child's Play to the Australian police.[10] [redacted]

[9] *See also* "Four Men Sentenced to Prison for Engaging in a Child Exploitation Enterprise on the Tor Network," Department of Justice (Aug. 12, 2019) (available at https://www.justice.gov/opa/pr/four-men-sentenced-prison-engaging-child-exploitation-enterprise-tor-network); Håkon F. Høydal, "Breaking the Dark Net: Why the Police Share Abuse Pics to Save Children," VG (Oct. 7, 2017), available at https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en.

[10] A special unit in the Australian police called Task Force Argos then ran Child's Play for 11 months. *See* Høydal, supra note 9.

[redacted]

Although the documents from [redacted] case are heavily redacted, there are multiple references to Homeland Security, as well as HSI Boston and a particular agent there - Special Agent Gregory Squire. *See* [redacted][11] It is clear that the investigation of multiple Tor hidden websites, including [redacted], relied heavily on collaboration between U.S. and foreign law enforcement. Canadian, U.S., New Zealand, and Australian law enforcement agencies worked together to investigate, locate, and arrest Faulkner and Falte. *See* [redacted] Høydal, supra note 9. U.S. law enforcement obtained information from those individuals, and then took that information to foreign law enforcement to continue the investigation into Tor hidden services sites. [redacted] Høydal, supra note 9. It was only because of that cooperation and collaboration that agents were able to identify and eventually arrest the creator of [redacted]

Other documents shed further light on the exact role of U.S. law enforcement in the investigation of target Tor hidden websites, including Website 2 ([redacted]), as a collaborative partner of foreign law enforcement agencies.

[11] HSI Boston and Special Agent Gregory Squire, who is based in Boston, appear to have played an important role in the investigation of the target Tor websites, including [redacted]. *See, e.g.,* Ex. 13, at ¶¶ 5-8; Ex. 15, at ¶ 62; Ex. 17, at ¶ 12.

First, a January 2017 FBI report documents a "preliminary investigation" into a Tor hidden service site with language identical to that found on [redacted]. *See* Ex. 18. This document establishes that the FBI opened an investigation into [redacted] more than two years before the IP addresses that had purportedly visited [redacted], *see* Ex. 1, 10-12, 15-16, were transmitted by a foreign law enforcement agency to U.S. law enforcement. Agent Moynihan withheld this information from her affidavit. Taken with the other facts counsel has since discovered about the extent to which U.S. law enforcement was involved in a joint venture with foreign law enforcement to investigate the website, Agent Moynihan's omission is significant.

Second, one of the attached affidavits states that U.S. law enforcement's investigation of multiple target websites on the Tor network was a "collaborative" effort with foreign law enforcement partners. *United States v. Thomas S. Clark*, Case No. 2:21-MJ-00147-JLW (W.D. Wash. Mar. 11, 2021) (Complaint) ("Clark Complaint") attached as Ex. 13, at ¶ 5. The Clark complaint clearly describes the same investigation that led to the identification of Mr. Kiejzo's IP address. Like Mr. Kiejzo's case, Clark involved a tip from an FLA that a specific IP address accessed a target website on the Tor network in April 2019. See Ex. 13, at ¶¶ 5-10. The language of the Clark complaint also mirrors that in Agent Moynihan's affidavit, especially in its description of the Tor network. *Compare* Ex. 13, ¶ 9, *with* Ex. 1, ¶¶ 13-14. In both cases, administrative subpoenas were sent to internet services providers (Comcast in Clark; Verizon in Kiejzo) and similar investigation was done to confirm who lived at the address. Ex. 13, ¶ 10; Ex. 1, ¶ 39. The "collaborative" investigation that formed the basis of the Clark case is therefore the same investigation that led to Mr. Kiejzo's IP address.

Third, in another case, HSI Boston is noted to have been working in tandem with foreign law enforcement to investigate Tor hidden services sites as early as 2018. *See United States v.*

Dashawn Webster, Case No. 2:18-CR-101-RAJ (E.D. Va. May 18, 2018) (Affidavit in Support of Application for Issuance of Criminal Complaint) ("*Webster* Complaint") attached as Ex. 17, at ¶ 13 ("HSI Boston is also conducting an investigation of various Darkweb sites **along with** foreign law enforcement partners.") (emphasis added). In fact, HSI Boston is specifically noted in several cases involving U.S.-FLA joint investigations outside of this District. *See* Ex. 13, at ¶¶ 5-8; Ex. 15, at ¶ 62; Ex. 17, at ¶ 12.

Fourth, the [redacted]'s own documents indicate that the investigation into Websites 2 and 3 was a partnership. Specifically, the [redacted] intelligence reports state that the material in the reports was disseminated to "international **partners** in receipt of [redacted] intelligence." Ex. 5.

[redacted]

[redacted]

Moreover, [redacted] reveals that U.S. law enforcement was able to search [redacted] for specific information, including account information, usernames, passwords, and related postings to those accounts, dating at least back to 2016. This information was available to U.S. law enforcement by January 2020, eight months before Agent Moynihan applied for the warrant in this case. However, Agent Moynihan did not include any information indicating what kind of activity, if any, Mr. Kiejzo had engaged in on that website. The absence of such information suggests that U.S. law enforcement in fact had no information that Mr. Kiejzo had engaged in any such activity when it applied for a warrant to search his home. Omitting this exculpatory evidence, which if included would have greatly undermined the tip's reliability, was material.

Together, these documents show that U.S. law enforcement's involvement in the investigation of [redacted] and other Tor hidden websites was much more significant and much more collaborative with foreign law enforcement partners than what was indicated in Agent Moynihan's affidavit. The materials reveal that U.S. law enforcement became aware of, and began investigating, [redacted] as early as 2016, when the website was created. From the outset of the investigation, U.S. law enforcement worked in tandem with foreign law enforcement agencies, including, at the very least, law enforcement in Canada, New Zealand, and Australia. HSI Boston appears to have played a significant role in that investigation. Finally, U.S. law enforcement appear

to have been in possession of a searchable copy of one of the target websites – [redacted] – since at least January 2020. The documents demonstrate that U.S. law enforcement has long been engaged in a joint venture with foreign law enforcement partners to investigate multiple Tor hidden services websites, including [redacted].

Likewise, the publicly available information about the [redacted] highlights the extent to which that particular agency regularly collaborates with U.S. law enforcement. The [redacted] is [redacted] law enforcement agency responsible for leading, supporting and coordinating the response to serious and organized crime.[12] [redacted]

[redacted].[13]

Although the Affidavit indicates that "U.S. law enforcement personnel did not participate in the investigative *work* through which [redacted] identified the IP address information provided by [redacted]," Ex. 1, ¶ 33, the [redacted] own representations about its collaborative work through its international liaison officers belie any conclusion that they solely engage in a simple information-sharing relationship with other countries. [redacted]

[12] *See* [redacted]

[13] *See* [redacted]

[redacted][14]

[redacted].[15]

[redacted]

[redacted][16]

[redacted][17]

Based on the scant materials made available to the defense by the government and the materials unearthed by the defense, it is clear there was a joint venture between the United States, [redacted], and other foreign law enforcement agencies to investigate target Tor websites, including Websites 2 and 3. Failing to include the extent to which U.S. law enforcement was engaged in this joint venture to investigate the target websites in Mr. Kiejzo's case was a significant and material omission. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012); *see also United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (finding that the defendant had made a *prima facie* showing, for purposes of motion to compel discovery, that the joint venture doctrine applied and that malware had been used to obtain the defendant's IP address where U.S. law enforcement worked with Australian and New Zealand authorities to uncover IP addresses in the United States).

---

[14] [redacted]

[15] *Id.*

[16] *See* [redacted]

See [redacted]

CONCLUSION

On its face, the affidavit fails to establish probable cause. Excising the myriad misrepresentations from the affidavit and adding in the information omitted from the affidavit, it is clear that no Magistrate, had she or he been presented with the reformed affidavit, would have found probable cause. For the above reasons, this Court should suppress all evidence and fruits obtained pursuant to the invalid search warrant and grant Mr. Kiejzo a *Franks* hearing.

Respectfully submitted,
VINCENT KIEJZO
By His Attorney,

/s/ Sandra Gant
Sandra Gant, BBO # 680122
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

/s/ Caitlin Jones
Caitlin Jones, MN ID # 0397519
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on June 1, 2022.

/s/ Sandra Gant
Sandra Gant